Managed by Fermi Research Alliance, LLC for the U.S. Department of Energy Office of Science

Demystifying Point Releases

Pat Riehecky
Linux at Fermilab
18 November 2015

Presentation Goals

The goal of this presentation is to demonstrate:

- The purpose of `5x`, `6x`, and `7x`
- Which updates are published to which locations
- It is the API/ABI that controls your runtime environment

Administrators use Point Releases for various reasons to accomplish many goals.

- Clarifying the content and behavior of Scientific Linux Point Releases should assist the systems administrator in determining how to achieve their computing goals.

Quick Facts on Naming

- `5.11` attempts to match Red Hat's release of RHEL5 update 11.
- `5rolling` is where we put testing releases.
  - It is not a place your production systems should utilize.
- `5x` is an **alias**, a symlink on the actual filesystem.
  - `5x` is **not** a release.
    - It points to whatever is "current".
      - Today, `5x` points to `5.11`.
      - Last year it pointed to `5.10`.
    - `5x` only exists because `5.11` exists and `5.10` existed before that.
    - When you try to install `5x`, you are really installing whatever it points to.

```
scientific/
├── 7.0
├── 7.1
└── 7x -> 7.1
```

```
fermi/
├── slf6.6
├── slf6.7
└── slf6x -> slf6.7
```

```
fermi/
├── slf510
├── slf511
└── slf5x -> slf511
```

Speaking of the `x` Tree

If your system has yum-conf-5x installed, then your yum updates are checking for updates in the `5x` alias.

Unless you've specifically removed it, you may have this package. If you don't want to be automatically upgraded to the next point release, by a `yum update` remove this package.

This is true for SL 5, SL 6, and SL 7
This is true for SLF 5, SLF 6, and SL 7 Fermilab Edition

Check your systems if this worries you!
In particular: 5.9+, 6.4+, 7.0+

Perhaps Some Larger Context

Before we go too far into Scientific Linux specifics,
let's take a look at other Operating Systems as a conceptual guide.

- Microsoft Windows collects some updates in Service Packs
  - Windows XP, XP SP1, XP SP2, XP SP3
    - And some security/bugfix updates are published outside of these
- Apple's MacOS collects some updates in Maintenance Updates
  - OS 10.9, 10.9.1, 10.9.2, 10.9.3
    - And some security/bugfix updates are published outside of these

- Scientific Linux has Point Releases
  - Point Releases are *similar* to these.
    - But unlike these others, the newest security errata is available even if you've not applied all published updates.

Clarifying Terms – A Point Release

- A Point Release:
  - Is a collection of packages
  - Matches upstream at time of release
    - SL 5.9 -> RHEL 5.9
    - SL 6.4 -> RHEL 6.4
    - SL 7.1 -> RHEL 7.1
  - Sets the expected features/Application Binary Interfaces (ABIs)
    - Each point comes with bug fixes and, typically, new features
    - One good definition of a Point Release:
      - The release that comes with Bug Fix X and Feature Y.
        - SL 5.10 includes fsfreeze, SL 5.9 does not
        - SL 6.7 includes python-six, SL 6.6 does not
        - SL 7.1 includes OverlayFS, SL 7.0 does not

Updating and Scientific Linux

Scientific Linux is based on Red Hat Enterprise Linux for a lot of reasons. One of them is the ABI policy.

- https://access.redhat.com/articles/rhel-abi-compatibility

… [An update] from Red Hat Enterprise Linux 6.1 to Red Hat Enterprise Linux 6.2, or a package update that fixes an identified security vulnerability, should not break the functionality of deployed applications as long as they adhere to standard Application Binary Interfaces (ABIs).

- From RHEL Solution 5154

When Red Hat releases an update or publishes a new point release for RHEL 6, it goes into the same repo with all of 6.0, 6.1, 6.2, etc.

The Anatomy of an Update and Updating

- An update is any or all of these:
  - security – patch ported from upstream
  - bug fix – ported from upstream
  - enhancement - backported upstream feature enhancement

- Red Hat classifies their updates as one and only one type
  - security, then enhancement, then bugfix
  - This means a security package may also contain an unrelated bugfix or enhancement.

- Via the `yum-security` plugin, Red Hat subscribers can choose to only install security updates (and required dependencies).
  - This behavior is similar to what Scientific Linux provides in the SL Point Releases

What Point Releases Are Not

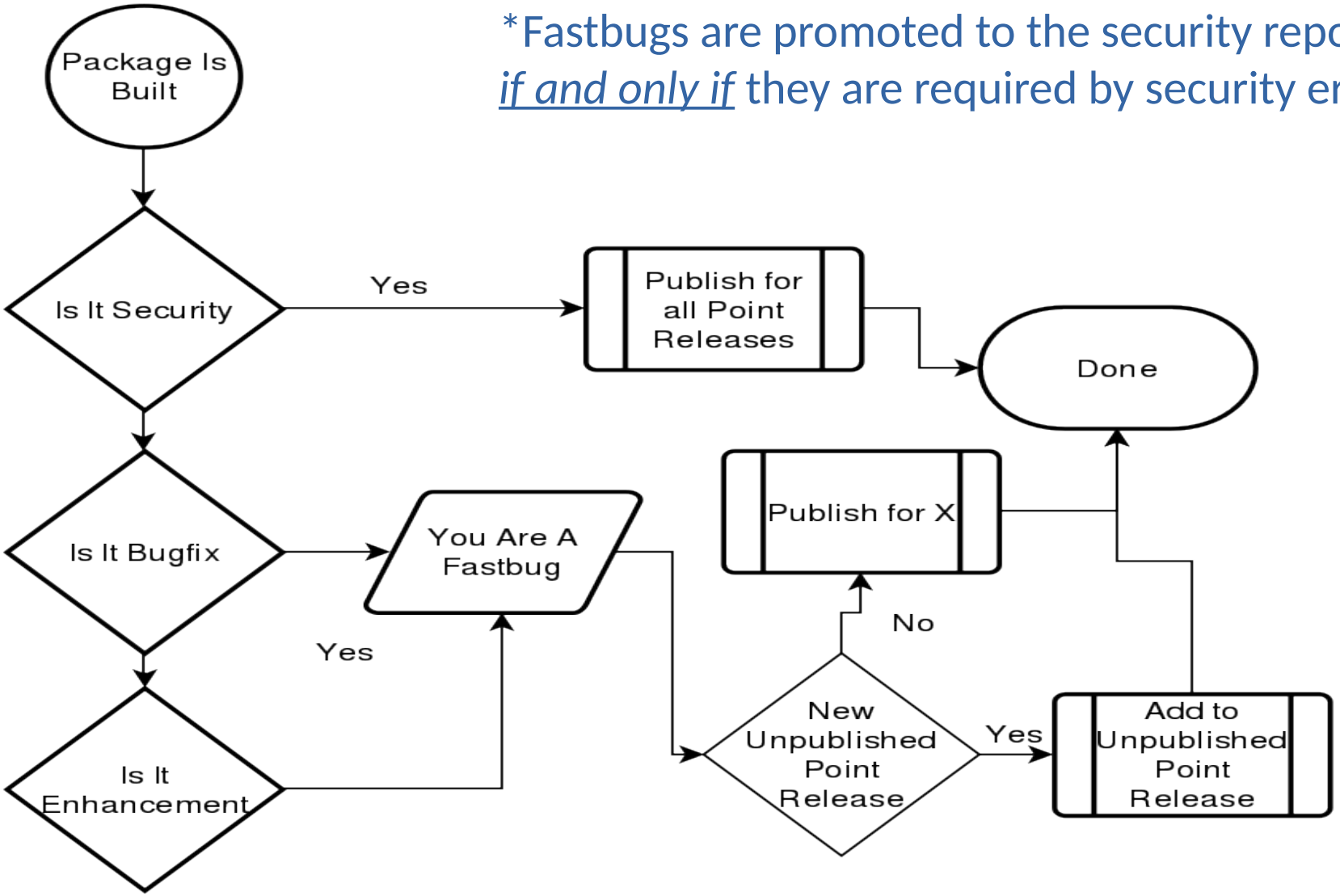
- A Scientific Linux Package includes **all** the security, bugfix, and enhancement code published by upstream in a given RPM.
  - Scientific Linux publishes packages in their entirety.
  - **We do not hand pick only the security patches out of Red Hat sources.**

If this is something you need, Red Hat sells a product called Extended Update Support (EUS).*

* EUS source is not published publicly

Errata Publishing for Scientific Linux* (Fermi)

*Fastbugs are promoted to the security repo *if and only if* they are required by security errata.



Errata Publication: Recap For Clarity - Security

- Where are security packages published?
  - Every point release should have the relevant security errata in its security repo.
- Is this similar to Red Hat's EUS product?
  - No, Scientific Linux publishes the updated packages as a whole, including **all** bugfix and enhancement code.
- Is this similar to updating a RHEL system with the `yum-security` plugin?
  - Yes, the `yum-security` plugin allows RHEL customers to install only security updates and their dependencies.

Errata Publication: Recap For Clarity - Fastbugs

- Where are fastbug packages published?
  - They are published in the fastbugs repo of the `X` release.
    - The fastbug repo is **DISABLED** by default in 5 and 6
    - The fastbug repo is **ENABLED** by default in 7
- Are fastbug packages pushed to older releases?
  - Only if they are `REQUIRED` for installing a security update.
- When will `5.3` receive the fastbug package from `5.11`?
  - When it is `REQUIRED` for a security errata – and not before.
- Is a fastbug package from `5.11` compatible with `5.3`?
  - Any SL 5 package should work on any SL5 system with the correct dependencies installed.

Errata Publication: Recap For Clarity – Edge Cases

- What are the current edge cases?
  - tzdata
    - Timezone changes may prevent logins from working due to clock skew, allow replay attacks, or confuse “realtime” data.
  - selinux-policy
    - Bugs in the selinux-policy may prevent software from working as expected, leaving you wanting to disable this security measure.
  - FNAL KERBEROS configs
    - These packages are special as failure to update them may prevent login to the host.

If you believe another package should be added to the list of edge cases, please open a ticket so we can discuss this further.

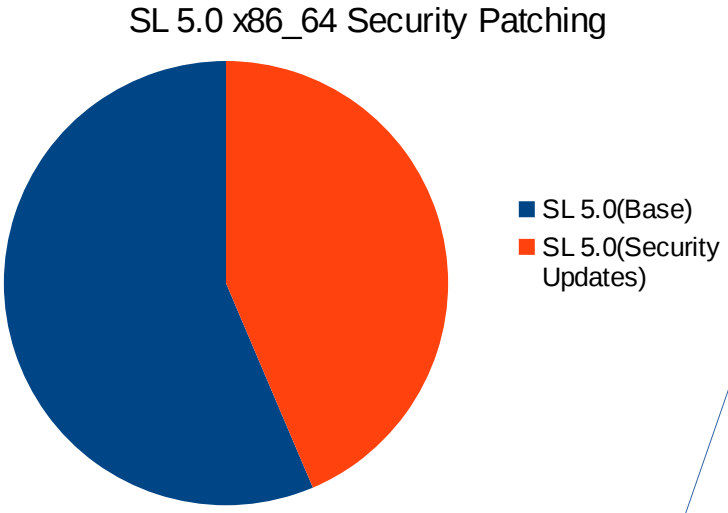
Errata Publication: Wrap up

- Now is probably a good time to pause for questions.

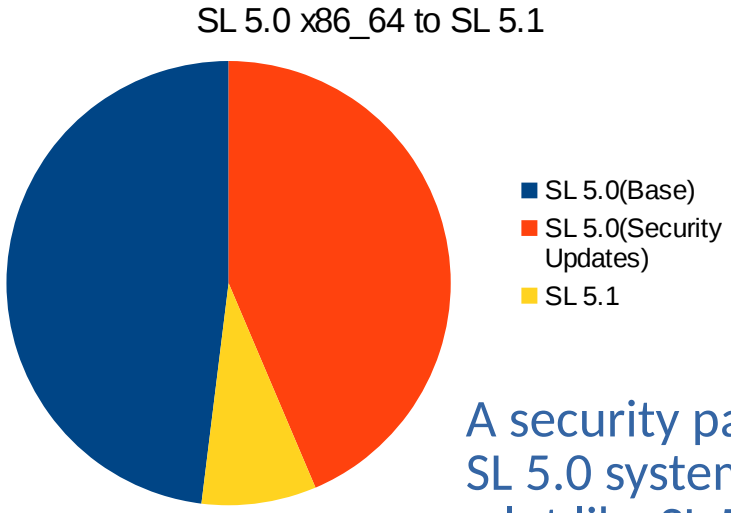
So Should I Just Run x?

- Well….
  - All updates come with risk.
    - The x tree has greater exposure to updates.
      - The x tree is always current, and what is current changes.
    - Aggressive testing can help lower your risk!

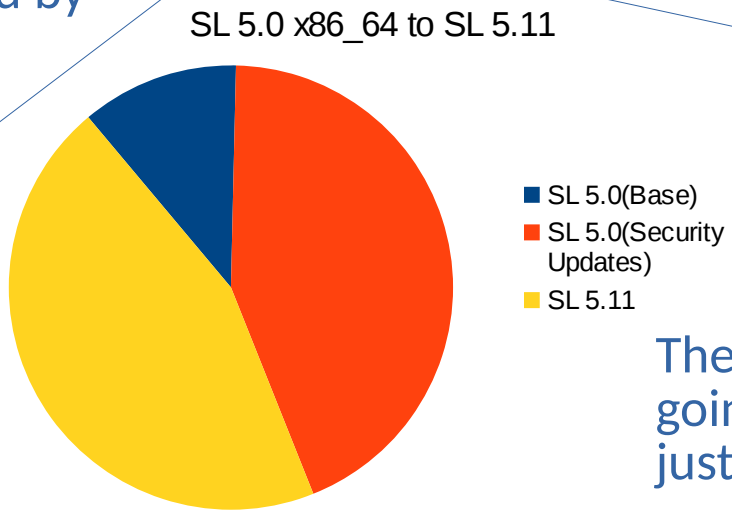
Let's Talk About Updates In Graph Form



Some SL 5.0 initial packages are updated by security errata.



A security patched SL 5.0 system looks a lot like SL 5.1.



There are more potential updates going from SL 5.0 to SL 5.11 then just security patching SL 5.0

Questions:

- Why are there no package names used as examples?
  - This is a conversation about “updates” as a whole, not the consequences of individual package changes.
- Should I run the `X` release, some other strategy, or ….?
  - You should test out what approach is best for your workload and your workflow.
    - The way SL publishes updates provides options.
- `/etc/redhat-release` says `5.1`, does that mean I'm running `5.1`?
  - `/etc/redhat-release` says your minimum expected feature set/ABI.
  - Updates installed on the system may provide additional features or introduce bugs breaking the older behavior.
  - This response does not answer yes or no to your question.

In Summary

- The `x` repo is just an alias – not a release
  - If you are concerned about automatically upgrading to the next release, make sure that `yum-conf-#x` is removed from your systems.
- We publish security updates and their necessary dependencies for older releases.
- We publish bugfix/enhancement packages to the `X` tree's fastbugs repo.
- The API/ABI your applications uses is what matters.
  - How you describe that, is up to you.
    - Point Release, Service Pack, Maintenance Update, etc.
- The one thing we can promise you is that software has bugs.
  - Updates aim to fix bugs, but sometimes they add new ones.
  - To find out whether those bugs affect you, you must test.

Your Questions?

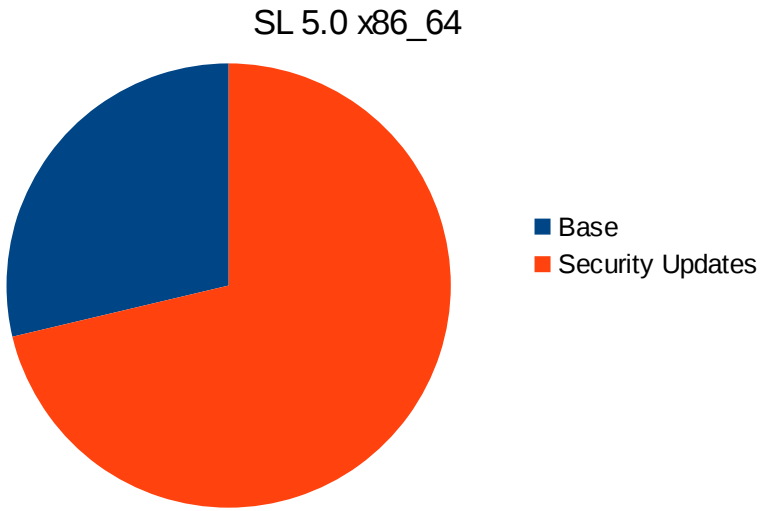
Supplementary Resources (not presented)

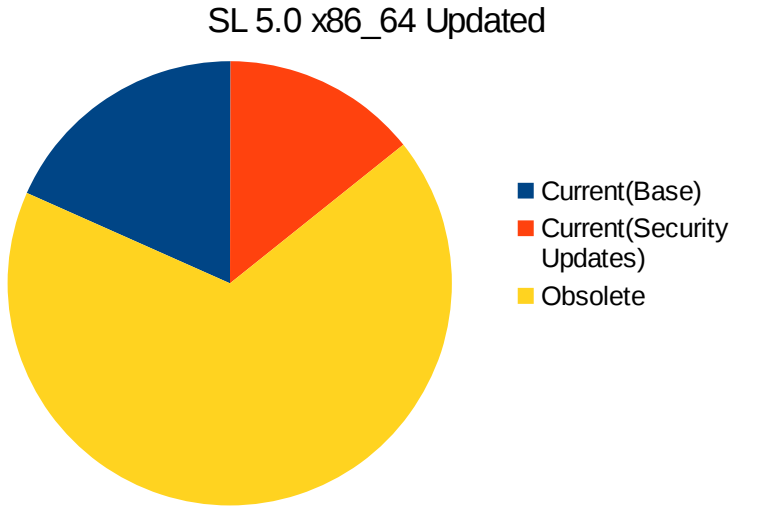
How The Graphs Were Made

- This experiment was conducted Nov 6 2015
  - on the x86_64 trees of SL 5.0, SL 5.1 and SL 5.11 using:
    - reposync -n, comm, and wc -l
- SL 5 is still receiving updates
  - Therefore, these numbers are for entertainment purposes only.
  - They will go out of date and will not be updated.
- The `kernel-module-*` packages were removed from consideration
  - They do not come from Red Hat and artificially inflate the numbers.
- Packages from the SL repo and the SL Security repo were used.
  - Fastbugs are disabled by default and, therefore, excluded.
- There is no system that could ever install 100% of the SL 5 packages.

Let's Talk About Updates: SL 5.0 x86_64

- 10967 packages in the default repos
- 3149 packages come from the base repo
- 7818 packages come from the security updates repo
- 2016 of the base packages are the “latest packages available for SL 5.0
- 1559 of the security updates are the “latest” packages available SL 5.0
- 7392 of the packages are “obsolete” for SL 5.0





Let's Talk About Updates: SL 5.0 x86_64 to Something Else

- Fully security patched, SL 5.0 has 3575 packages
  - 2016 from base
  - 1559 from security updates.
- Updating to SL 5.1 from the fully security patched SL 5.0 system upgrades 298 packages
- Updating to SL 5.11 from the fully security patched SL 5.0 system upgrades 1606 packages